(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33336 A1

(51) International Patent Classification[7]: G06F 9/00, 9/46, 11/30, 12/14, 15/16, 15/163, 17/60, H04K 1/00, H04L 9/00, 9/32

(21) International Application Number: PCT/US00/25573

(22) International Filing Date:
18 September 2000 (18.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/430,859 29 October 1999 (29.10.1999) US

(71) Applicant *(for all designated States except US)*: **ZAP ME!** [US/US]; 3000 Executive Parkway, Suite 150, San Ramon, CA 94583 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **STRASNICK, Steven, L.** [US/US]; 366 Sierra Vista Avenue, Unit #15, Mountain View, CA 94043 (US).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th floor, 7th Floor, Los Angeles, CA 90025 (US).

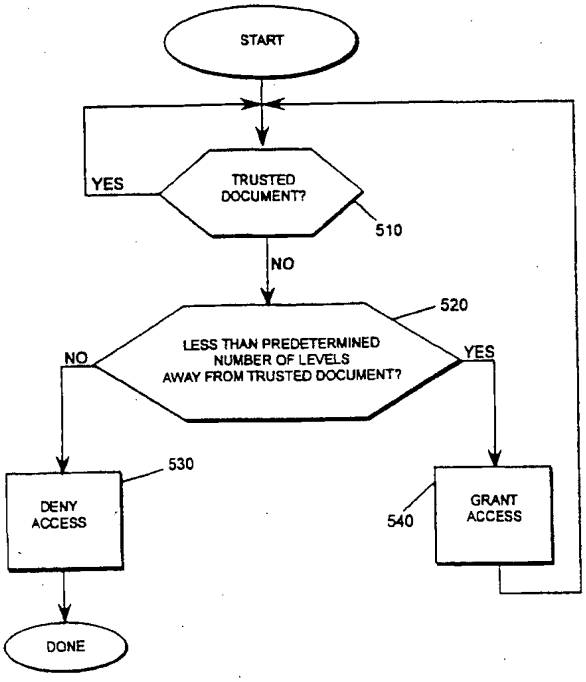
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: LEVEL-BASED NETWORK ACCESS RESTRICTION



(57) Abstract: Methods and apparatuses for level-based network access restriction are described. A user of network resources logs on to the network according to any appropriate security procedure. The user is provided access to a known, trusted resource (510) as a starting point. From the starting point, the user can access other network resources by following links from the starting point or in another manner. The network resources accessed by the user are analyzed to determine whether the resource is a trusted resource (510). If the resource is a trusted resource (510), the user is allowed (540) to follow a predetermined number of links away from the trusted resource before access is denied (530).

WO 01/33336 A1

LEVEL-BASED NETWORK ACCESS RESTRICTION

FIELD OF THE INVENTION

The invention relates to network access restrictions. More particularly, the invention relates to methods and apparatuses for limiting the levels of access away from a trusted network resource.

BACKGROUND OF THE INVENTION

In many situations, organizations, such as schools and public libraries, desire to provide network access to many individuals having many different needs. This access is typically the Internet; however, access to other networks can also be provided. In certain environments, such as schools and public libraries, many of the individuals that desire network access are minors, and it is desirable to provide somewhat restricted access to the network (e.g., no access to pornographic World Wide Web sites).

Many schemes have been developed to provide acceptable restricted access to networks. Typical network restriction schemes include user name and password access restriction and/or approved/restricted resource lists. User name and password schemes require a user to provide an authorized user name and password to access network resources (e.g., a World Wide Web page, an audio file, a text document). However, user name and password schemes can be easily defeated if an authorized user provides his/her authorized user name and password to others.

Approved/restricted resource list schemes maintain an approved list and/or a restricted list that list approved network resources and restricted network resources,

respectively. In order for a user to have access to a particular network resource, the resource must be included in the approved list and/or not included in the restricted list, depending on how the access scheme is implemented. However, with large, constantly changing networks such as the World Wide Web, maintaining access and/or restricted lists for multiple users generally does not provide a satisfactory network access experience for users and is difficult and time consuming to maintain for network access providers.

What is needed in an improved scheme for restricting access to network resources.

SUMMARY OF THE INVENTION

Methods and apparatuses for level-based network access restriction are described. A browser or other application determines whether an electronic document is a trusted electronic document. Access to further electronic documents is limited to a predetermined number of levels away from the trusted electronic document. In one embodiment, access to the further electronic documents is accomplished via electronic links. Further access is denied if the electronic document is not a trusted electronic document.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is illustrated by way of example, and not by way of limitation in the figures of the accompanying drawings in which like reference numerals refer to similar elements.

Figure 1 illustrates one embodiment of a computer system.

Figure 2 illustrates one embodiment of a network configuration.

Figure 3 illustrates one embodiment of a network operations center coupled to a network.

Figure 4 is a conceptual block diagram of electronic documents having links to further electronic documents.

Figure 5 is a flow diagram of one embodiment of level-based network access restrictions.

DETAILED DESCRIPTION

Methods and apparatuses for level-based network access restriction are described. In the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

Some portions of the detailed descriptions which follow are presented in terms of algorithms and symbolic representations of operations on data within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following

discussion throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be

appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

In general, a user of network resources logs on to a network according to any appropriate security procedure. The user is provided access to a known, trusted resource (e.g., document, file) as a starting point. From the starting point, the user can access other network resources by following links from the starting point or in another manner. The network resources accessed by the user are analyzed to determine whether the resource is a trusted resource. If the resource is a trusted resource, the user is allowed to follow a predetermined number of links away from the trusted resource before access is denied.

Figure 1 illustrates one embodiment of a computer system. The computer system of Figure 1 can be used in various capacities with the present invention. For example, the computer system can be a terminal used by a user to access local or remote resources, the computer system can be a server providing remote access to a resource, or the computer system can be a proxy server providing access to remote computer systems.

Computer system 100 includes bus 101 or other communication device for communicating information and processor 102 coupled to bus 101 for processing information. Computer system 100 further includes random access memory (RAM) or other dynamic

storage device 104 (referred to as main memory), coupled to bus 101 for storing information and instructions to be executed by processor 102. Main memory 104 also can be used for storing temporary variables or other intermediate information during execution of instructions by processor 102. Computer system 100 also includes read only memory (ROM) and/or other static storage device 106 coupled to bus 101 for storing static information and instructions for processor 102. Data storage device 107 is coupled to bus 101 for storing information and instructions.

Data storage device 107 such as a magnetic disk or optical disc and corresponding drive can be coupled to computer system 100. Computer system 100 can also be coupled via bus 101 to display device 121, such as a cathode ray tube (CRT) or liquid crystal display (LCD), for displaying information to a computer user. Alphanumeric input device 122, including alphanumeric and other keys, is typically coupled to bus 101 for communicating information and command selections to processor 102. Another type of user input device is cursor control 123, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor 102 and for controlling cursor movement on display 121.

Computer system 100 further includes network interface 130 to provide access to a network, such as a local area network. One embodiment of the present invention is related to the use of computer system 100 to provide network access having level-based restrictions. According to one embodiment, network access having level-based restrictions is provided by one or more computer systems or other electronic devices in response to one or more processors executing sequences of instructions contained in memory.

Instructions are provided to memory from a storage device, such as magnetic disk, a read-only memory (ROM) integrated circuit, CD-ROM, DVD, via a remote connection (e.g., over a network via network interface 130), etc. In alternative embodiments, hard-wired circuitry can be used in place of or in combination with software instructions to implement the present invention. Thus, the present invention is not limited to any specific combination of hardware circuitry and software instructions.

Figure 2 illustrates one embodiment of a network configuration. The configuration of Figure 2 is described in terms of both land based communications and satellite communications; however, the manner of communication is not central to the present invention. Therefore, the present invention is applicable to any interconnection of devices that provide access to local and remote resources.

Wide area network 200 provides an interconnection between multiple local area networks (e.g., 220 and 230), individual terminals (e.g., 260) and one or more network operations centers (e.g., 250). In one embodiment, wide area network 200 is the Internet; however, any wide area network (WAN) or other interconnection can be used to implement wide area network 200.

Terminal 260 is an individual terminal that provides access to network resources as well as local resources for a user thereof. In one embodiment, terminal 260 is a personal computer connected to wide area network 200 via a modem, a wireless connection, etc. Alternatively, terminal 260 can be a set-top box such as a WebTV™ terminal available from Sony Electronics, Inc. of Park Ridge, New Jersey, or a set-top box using a cable modem to access a network such as the Internet. Similarly, terminal 260 can be a "dumb" terminal or a

thin client device such as the ThinSTAR™ available from Network Computing Devices, Inc. of Mountain View, California.

Local area network 220 provides an interconnection of devices at a local level. For example, local area network 220 can interconnect multiple computers, printers, and other devices within one or more buildings. Local area network 220 is coupled to wide area network 200. Similarly, local area network 230 provides an interconnection of devices. However, local area network 230 is coupled to satellite communications devices 240 as well as wide area network 200.

Network operations center 250 is coupled to wide area network 200 and provides access to network resources for terminal 260, local area network 220 and local area network 230. Communication between network communications center 250 and either terminal 260 or local area network 220 is accomplished by wide area network 200. As described in greater detail below, network operations center 250 and local area network 230 communicate via wide area network 200 and/or satellite communications devices 240.

In one embodiment network operations center 250 includes multiple servers (not shown in Figure 2) that provide access to network and other resources. For example, network operations center 250 can include a Web proxy server that provides access to the World Wide Web (WWW, or the Web) for devices of local area network 220, local area network 230 and terminal 260. Network operations center 250 can also include other devices, such as a middleware server or a file server that provide information to devices coupled to network operations center 250.

In one embodiment, information is communicated between network operations center 250 and local area network 230 via uni-cast, multicast or broadcast satellite communications devices 240, which includes necessary components to provide communications between network operations center 250 and local area network 230. In one embodiment, satellite communication are accomplished using Transmission Control Protocol/Internet Protocol (TCP/IP) embedded within a digital video broadcast (DVB) stream; however, alternative communication protocols can be used. In one embodiment, satellite communications are bi-directional. Alternatively, if satellite communications are uni-directional, wide area network 200 can be used to provide a hybrid, asymmetric bi-directional communications system such as the SkySurfer™ platform available from Gilat Satellite Networks, Inc. of McLean, Virginia.

Figure 3 illustrates one embodiment of a network operations center coupled to a network. With respect to description of Figure 3, wide area network 200 and satellite communications devices 240 are implemented as described above in Figure 2. Notwithstanding being described as including certain types of servers and other devices, network operations center 250 can include different or additional components as well as multiple components, for example, multiple Web servers. Each server can be one or more software and/or hardware components.

Network operations center (NOC) 250 provides resources to local area networks and individual terminals (not shown in Figure 3) as well as a gateway to a larger network such as the Internet. Thus, network operations center 250 can be used to provide a controlled set of resources while being part of a larger network. This is particularly advantageous in

situations where users of the local area networks are somewhat homogenous. For example, students in similar grade levels, professionals, and other groups.

Additional uses and details of the network of Figure 2 and the network operations center of Figure 3 can be found in U.S. Patent application number 09/216,016, entitled "OPTIMIZING BANDWIDTH CONSUMPTION FOR DOCUMENT DISTRIBUTION OVER A MULTICAST ENABLED WIDE AREA NETWORK" and U.S. Patent application number 09/216,018, entitled "A METHOD AND APPARATUS FOR SUPPORTING A MULTICAST RESPONSE TO A UNICAST REQUEST FOR DATA," both of which are assigned to the corporate assignee of the invention.

NOC router 300 is coupled to NOC LAN 305 and provides routing and firewall functionality for the servers and other components of network operations center 250. NOC router 300 can be implemented in any manner known in the art. In one embodiment, database 360 is coupled to NOC LAN 305. Database 360 can be used, for example, to store information about authorized users of associated local area networks, or to store information about resources that are available on each terminal connected to the network.

Database 360 can also be used to store statistics about network usage, advertisement media assets to be downloaded to devices of the local area networks, etc. In one embodiment database 360 is used to store user profile information for authorized users of the network. Data store 365 represents data stored by database 360 and can be one or more physical devices and logical data tables.

Master proxy server 370 is also coupled to NOC LAN 305 to provide World Wide Web resources to devices of the connected local area network(s) or individual terminals. In

one embodiment web server 310 is a Hypertext Markup Language (HTML) and/or Secure Sockets Layer (SSL) server. Of course, Web server 310 can be another type of server (e.g. FTP, multicast "carousel" data broadcast server, reliable file multicast server, UNIX host, media server, etc.). Web cache 320 is used to store Web resources (e.g., Web pages) that are most often accessed, most recently accessed, etc. In one embodiment, Web cache 320 stores a predetermined set of Web resources that are provided to the local area networks. In a school network environment, the cached Web resources can be, for example, a preapproved set of Web pages. In one embodiment all or a portion of the contents of Web cache 320 are replicated on local networks.

Middleware server 330 manages database applications and interfaces with other servers in network operations center 250. For example, middleware server 330 can determine which users have access to Web server 310 and grant access accordingly. Middleware server 330 can also dynamically generate a Web page, graphic or chart based on database content. In addition, middleware server 330 can acquire and process/evaluate data from a plurality of database servers and logical databases.

Middleware server 330 can also be replicated on local area networks, such as local area networks 220 and 230 of Figure 2. Middleware server 330 can be executed in any sufficient manner known to the art, for example, WebObjects® available from Apple Computer, Inc. of Cupertino, California, or a similar database middleware product. Alternatively, each client and server can act as its own middleware device by interfacing with the database servers on their own behalf though existing database interfacing technologies such as the Common Object Request Broker Architecture (CORBA) as defined

by Object Management Group, Inc. of Framingham, Massachusetts or COM+ available from Microsoft Corporation of Richmond, Washington.

Application server 340 provides applications programs to devices coupled to network operations center 250. Application server 340 conceptually represents two different types of servers. Application server 340 can be part of a client-server architecture where the server provides data to a client (e.g., HTML server, e-mail server, bulletin board server). Application server 340 can also be a software distribution and management server for "stand alone" programs. Master proxy server 370 provides World Wide Web access to devices coupled to network operations center 250. Master proxy server 370 can be implemented in any manner known in the art.

Figure 4 is a conceptual block diagram of electronic documents having links to further electronic documents. The example of Figure 4 is described in terms of documents; however, access restrictions to any network resources can be provided as described herein. The documents of Figure 4 can be in any appropriate format, for example, Hypertext Markup Language (HTML), extensible Hypertext Markup Language (XHTML), extensible markup language (XML), etc. Also, the documents of Figure 4 can be multiple pages from a single Web site. For example, an index page may be trusted, but other pages of the same Web site may not be designated as trusted documents.

Document 400 provides a starting point for network access. In one embodiment, all users are provided a trusted document as a starting point for network access. Document 400 can be accessed, for example, by a browser application running on a computer system. The trusted document may be different for different users. In one embodiment, document 400 is

an index document that provides links to other documents. For example, document 400 can have an index of links to documents on approved or appropriate material, determined based on, for example, information known (e.g., age, location, time of day) about the user, the environment and/or the purpose of the network access.

In one embodiment, all users of a particular local network are provided the same starting document that can be used to access a larger network. For example, in a school environment, the school can have a private local network to which student computers are connected. The students can access other networks, for example, the Internet, with the computers. When the students log on the local network a known, trusted document (e.g., a school-provided index page) is provided as a starting point for navigation.

Document 400 includes one or more electronic links (e.g., link 402, link 404, link 408). The links can point to trusted documents, unknown documents and/or untrusted documents. The list of untrusted documents is not necessary, but may be useful in preventing access to documents that would otherwise be accessible. In one embodiment, a list of trusted documents and/or a list of untrusted documents is maintained. In alternative embodiments, the browser application analyzes a document to determine whether the document should be trusted.

In the example of Figure 4, link 402 points to untrusted document 410. If an untrusted document list is maintained, access to untrusted document 410 is denied. If an untrusted document list is not maintained, access to untrusted document 410 is granted if the user is allowed to access documents linked to document 400 and untrusted document 410 is within the predetermined number of allowed levels away from a trusted document.

In one embodiment, the browser application running on the user's computer system tracks the status of documents accessed and allows or denies access to linked documents based on a predetermined number of levels away from a trusted document the user is allowed to access. In alternate embodiments, other applications, for example, a middleware server in a NOC (not shown in Figure 4) can be used to allow or deny access to documents. In one embodiment, the browser application allows or denies access to electronic documents based on information (e.g., a trusted document list) retrieved from the NOC.

In one embodiment, a user is allowed to follow links one level away from trusted documents. In such an embodiment, untrusted document 410 is accessible to the user, but no links (not shown in Figure 4) included in untrusted document 410 can be followed. In an alternate embodiment, a user is allowed to follow links two levels away from trusted documents. In such an embodiment, the user can follow links from untrusted document 410 to another document (not shown in Figure 4), but no links from the second document. Any number of levels can be used; however, the greater the number of levels allowed, the less restrictive the network access becomes.

Link 404 points to unknown document 420. If the user is limited to one level away from a trusted document, the links (e.g., link 422 and link 428) to unknown document 440 and trusted document 450 from unknown document 420 are denied. If multiple levels are allowed, the link to unknown document 440 can be followed as described above. The link to trusted document 450 can also be followed. Because document 450 is trusted, the predetermined number of levels allowed to the user are reset and the user can follow the predetermined number of levels away from trusted document 450.

In the example of Figure 4, document 400 also includes link 408 to trusted document 430. Because the link takes the user from one trusted document to another, the user is allowed to follow the predetermined number of levels away from trusted document 430. For example, the user can follow link 432 to unknown document 460. If multiple levels are allowed, the user can follow link 462 from unknown document 460 to unknown document 470.

Figure 5 is a flow diagram of one embodiment of level-based network access restrictions. Access to trusted documents is granted at 510. Access restrictions are not imposed on a user if the user is accessing only trusted documents. In one embodiment, a browser application determines whether a document is a trusted document; however, other applications can determine whether a document is a trusted document.

If a document is not a trusted document at 510, the browser determines whether the document is less than a predetermined levels away from a trusted document at 520. If not, access is denied at 530. If the document is less than the predetermined number of levels away from a trusted document at 520, access is granted to the requested document at 540. The process of 510, 520, 530 and 540 is repeated for subsequent documents.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes can be made thereto without departing from the broader spirit and scope of the invention. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A method comprising:

determining whether an electronic resource is a trusted electronic resource;

limiting access to further electronic resources to a predetermined number of levels away from the trusted electronic resource, wherein access to the further electronic resources is accomplished via electronic links; and

denying further access if the electronic resource is not a trusted electronic resource.

2. The method of claim 1 wherein the electronic resource comprises a World Wide Web page.

3. The method of claim 1 wherein the electronic resource comprises a Hypertext Markup Language (HTML) document.

4. The method of claim 1 wherein the electronic resource comprises a Virtual Reality Markup Language (VRML) document.

5. The method of claim 1 wherein the trusted electronic resource is an index document.

6. The method of claim 1 wherein the predetermined number of levels away from the trusted resource comprises following an electronic link to a second resource having additional electronic links, wherein following the additional electronic links from the second resource is prohibited.

7. The method of claim 1 wherein the predetermined number of levels away from the trusted electronic resource comprises following an electronic link to a second electronic resource having additional electronic links and following one of the links from the second resource to a third resource, wherein following the additional electronic links from the third resource is prohibited.

8. A machine-readable medium having stored thereon sequences on instructions that when executed by one or more processors cause one or more electronic devices to:

determine whether an electronic resource is a trusted electronic resource;

limit access to further electronic resources to a predetermined number of levels away from the trusted electronic resource, wherein access to the further electronic resources is accomplished via electronic links; and

deny further access if the electronic resource is not a trusted electronic resource.

9. The machine-readable medium of claim 8 wherein the electronic resource comprises a World Wide Web page.

10. The machine-readable medium of claim 8 wherein the electronic resource comprises a Hypertext Markup Language (HTML) document.

11. The machine-readable medium of claim 8 wherein the electronic resource comprises a Virtual Reality Markup Language (VRML) document.

12. The machine-readable medium of claim 8 wherein the trusted electronic resource is an index document.

13. The machine-readable medium of claim 8 wherein the predetermined number of levels away from the trusted resource comprises following an electronic link to a second resource having additional electronic links, wherein following the additional electronic links from the second resource is prohibited.

14. The machine-readable medium of claim 8 wherein the predetermined number of levels away from the trusted electronic resource comprises following an electronic link to a second electronic resource having additional electronic links and following one of the links from the second resource to a third resource, wherein following the additional electronic links from the third resource is prohibited.

15. An apparatus comprising:

means for determining whether an electronic resource is a trusted electronic resource;

means for limiting access to further electronic resources to a predetermined number of levels away from the trusted electronic resource, wherein access to the further electronic resources is accomplished via electronic links; and

means for denying further access if the electronic resource is not a trusted electronic resource.

16. The apparatus of claim 15 wherein the predetermined number of levels away from the trusted resource comprises following an electronic link to a second resource having additional electronic links, wherein following the additional electronic links from the second resource is prohibited.

17. The method of claim 15 wherein the predetermined number of levels away from the trusted electronic resource comprises following an electronic link to a second electronic resource having additional electronic links and following one of the links from the second resource to a third resource, wherein following the additional electronic links from the third resource is prohibited.

18. A network comprising:

a first device to store electronic resources having links; and

a second device coupled to the first device, the second device executing a browser application to access electronic resources, wherein the browser determines a trusted status of an electronic resource to be accessed, and further wherein the browser limits access to further electronic resources to a predetermined number of levels away from a trusted electronic resource.

19 The network of claim 18 further comprising a third device to store electronic resources having links, the third device coupled to the first device and to the second device, wherein at least one of the links in the electronic resources of the first device indicate one of the electronic resources of the third device, and further wherein the browser limits access to the trusted electronic resource of the first device and to the electronic resources of the third device indicated by the links in the electronic resources of the first device.

20. The network of claim 18 further comprising:

a third device coupled to the first device and to the second device, the third device to store electronic resources having links, wherein one of the links in the electronic resources of the first device indicates one of the electronic resources of the third device; and

a fourth device coupled to the second device and to the third device, the fourth device to store electronic resources, wherein one of the links in the resources of the third device indicates one of the electronic resources of the fourth device, and further wherein the browser limits access to the trusted electronic resource of the first device, to the electronic resource linked to the trusted electronic resource of the first device, and to the electronic

resource of the fourth device linked to the electronic resource of the third device linked to the trusted electronic resource of the first device.

21. The network of claim 18 wherein one or more of the devices comprises a computer system.

22. The network of claim 18 wherein one or more of the devices comprises a set-top box.

23. The network of claim 18 wherein one or more of the devices is an electronic personal digital assistant (PDA).

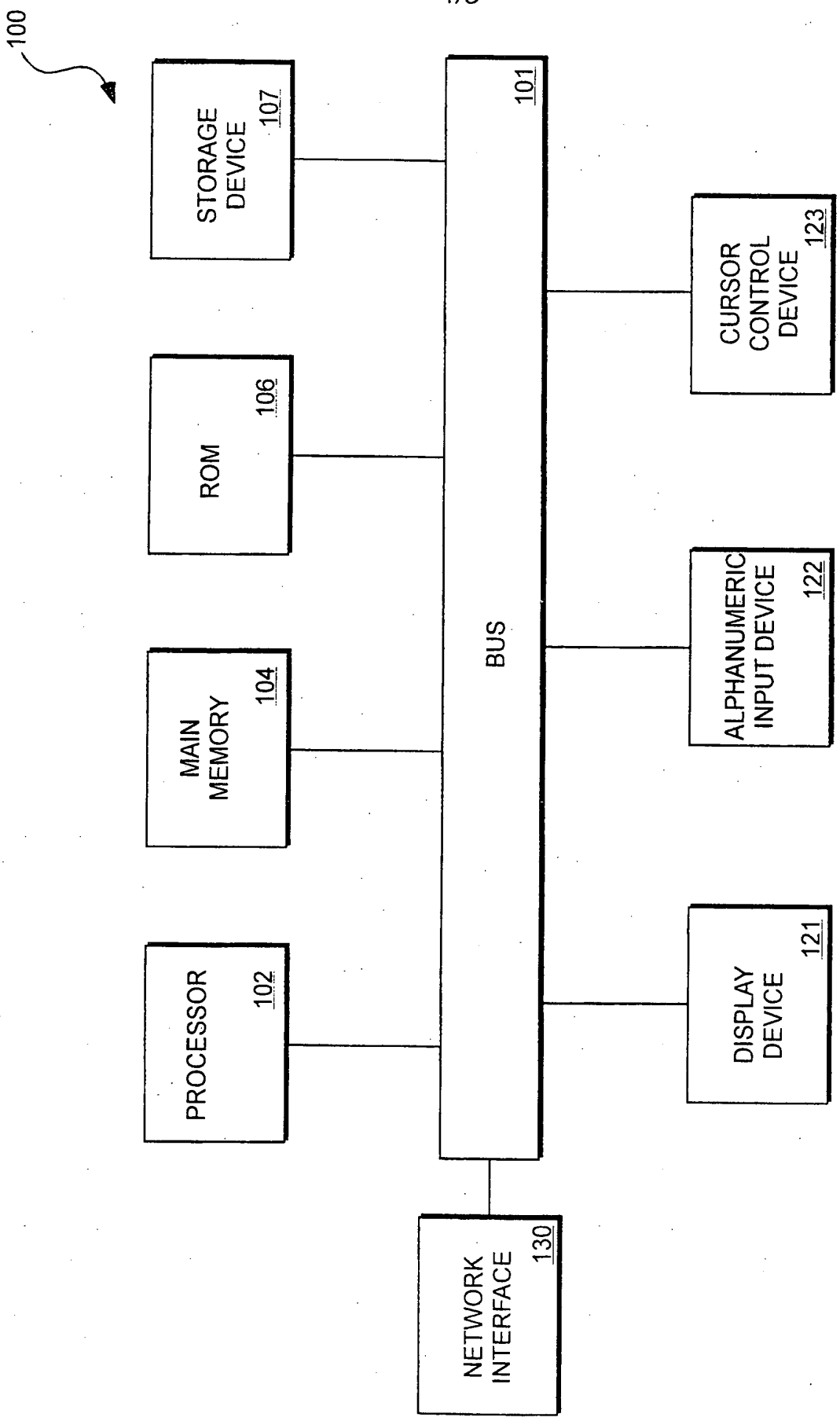


FIG. 1

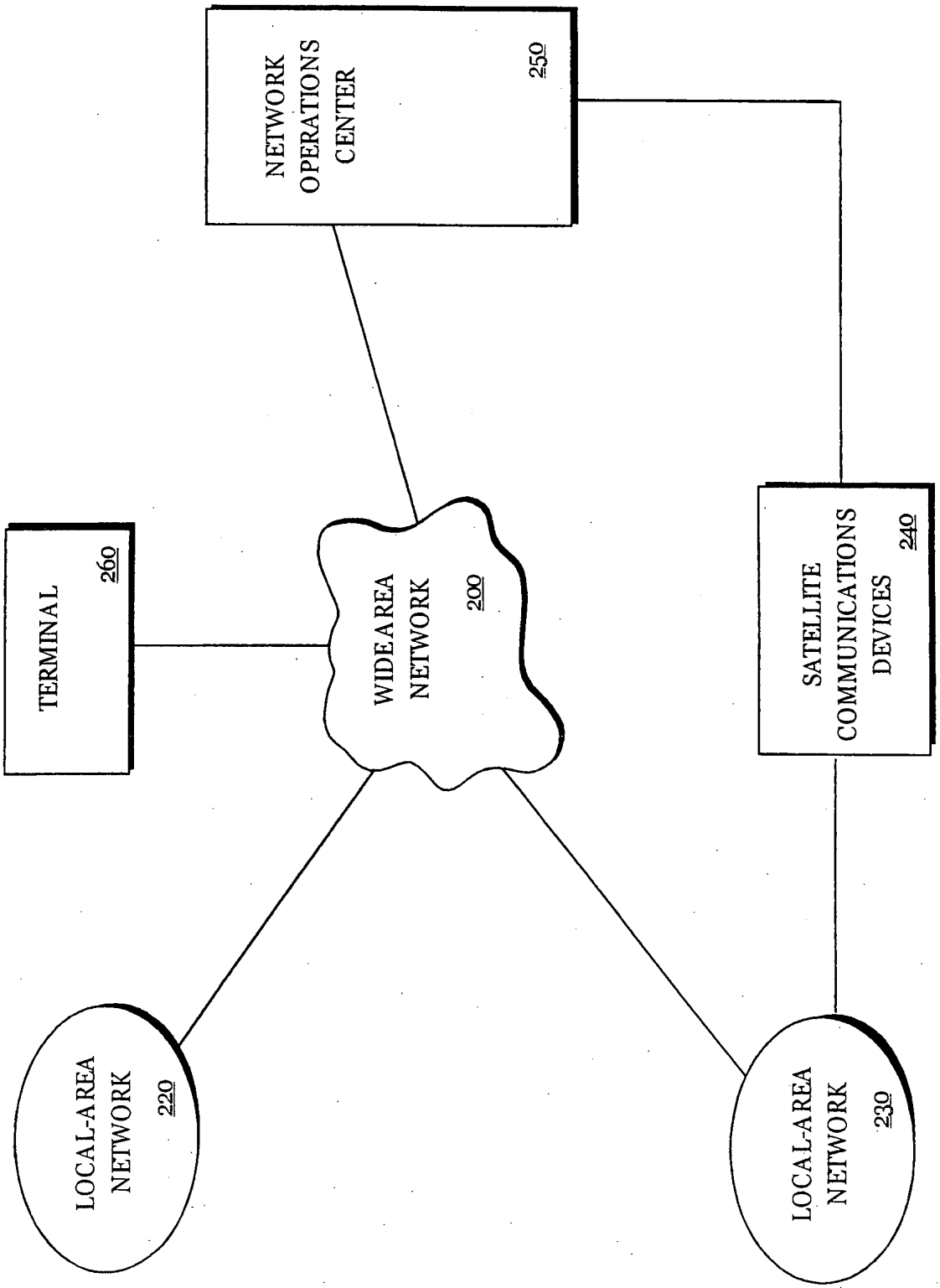


FIG. 2

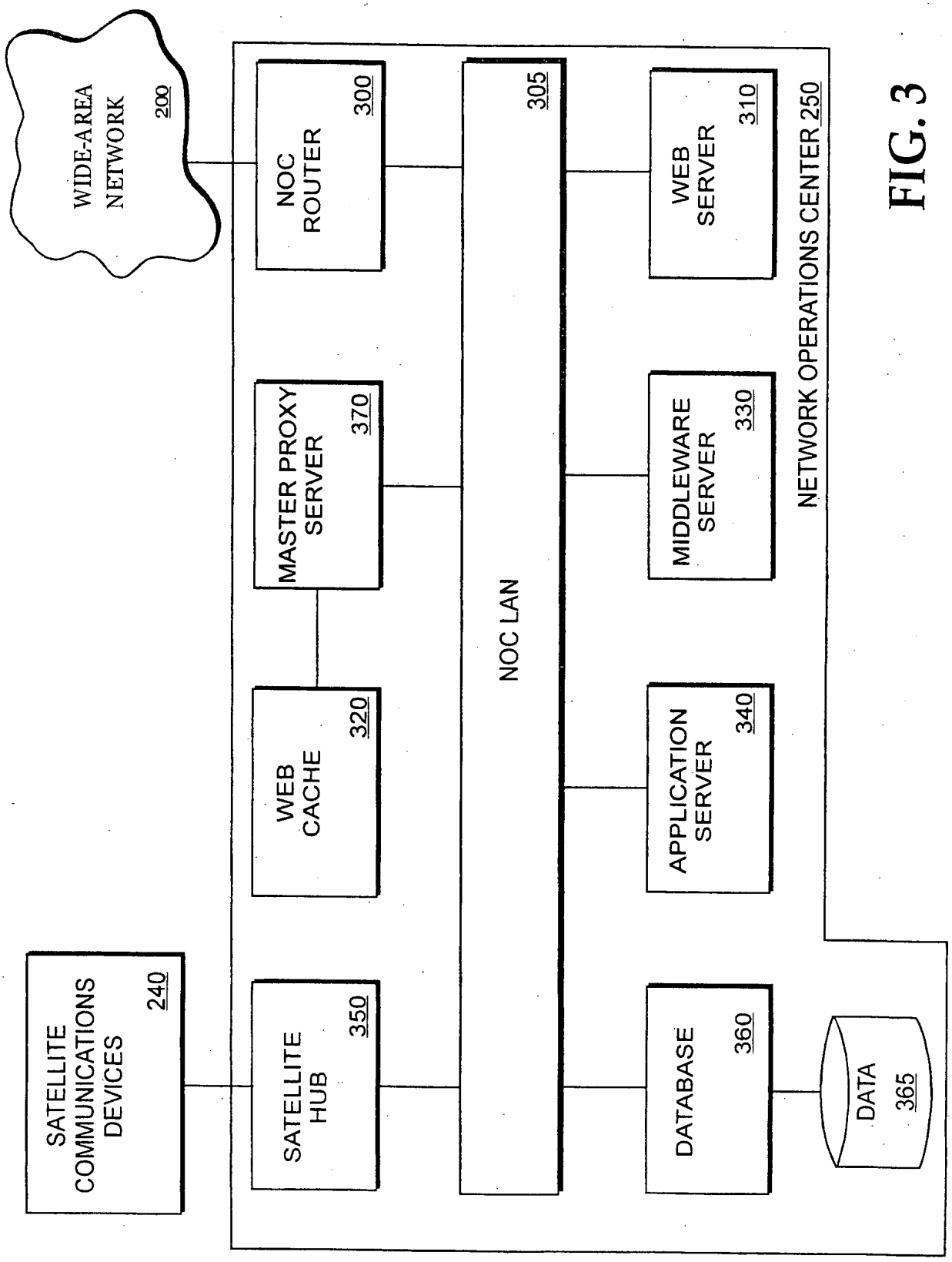


FIG. 3

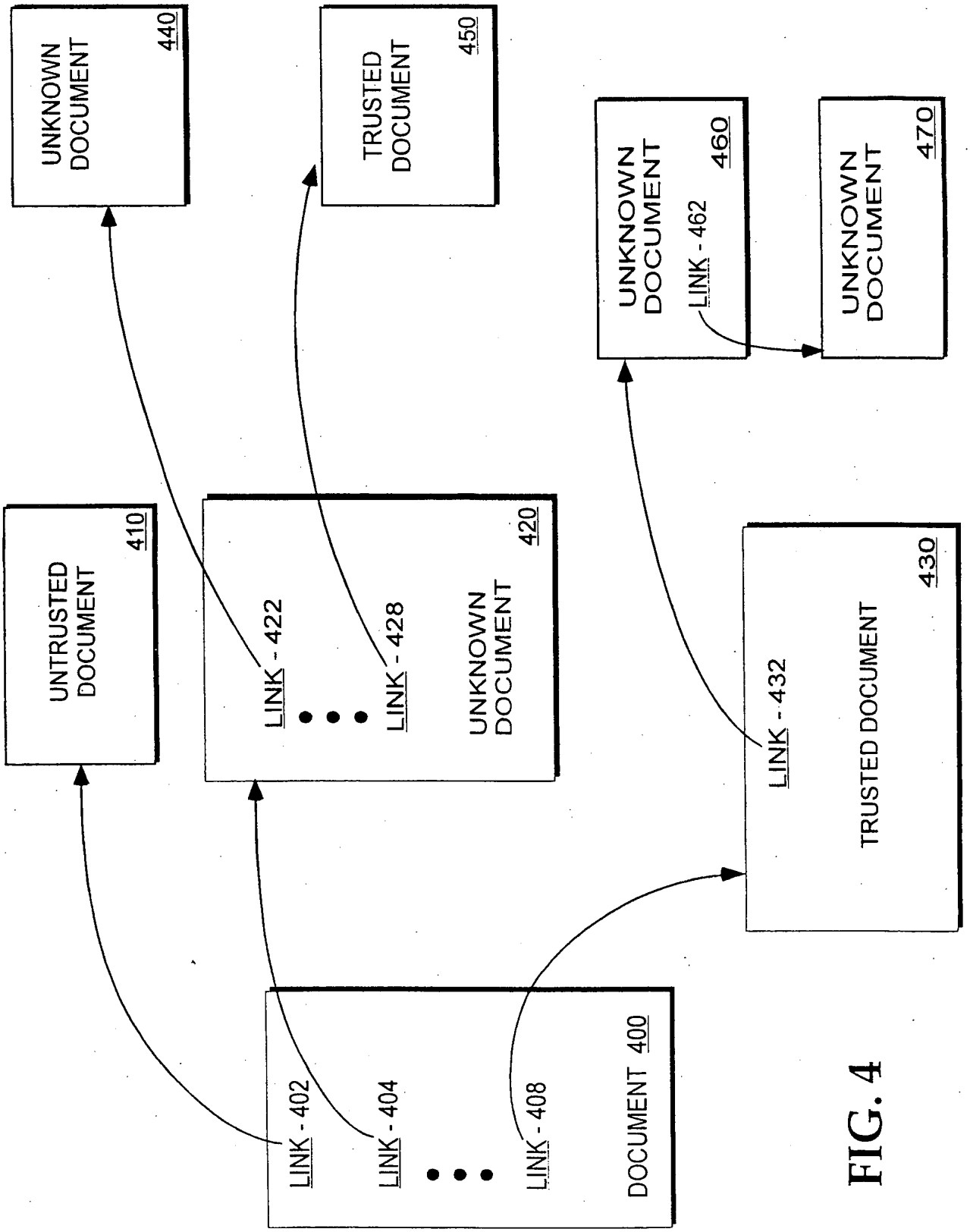


FIG. 4

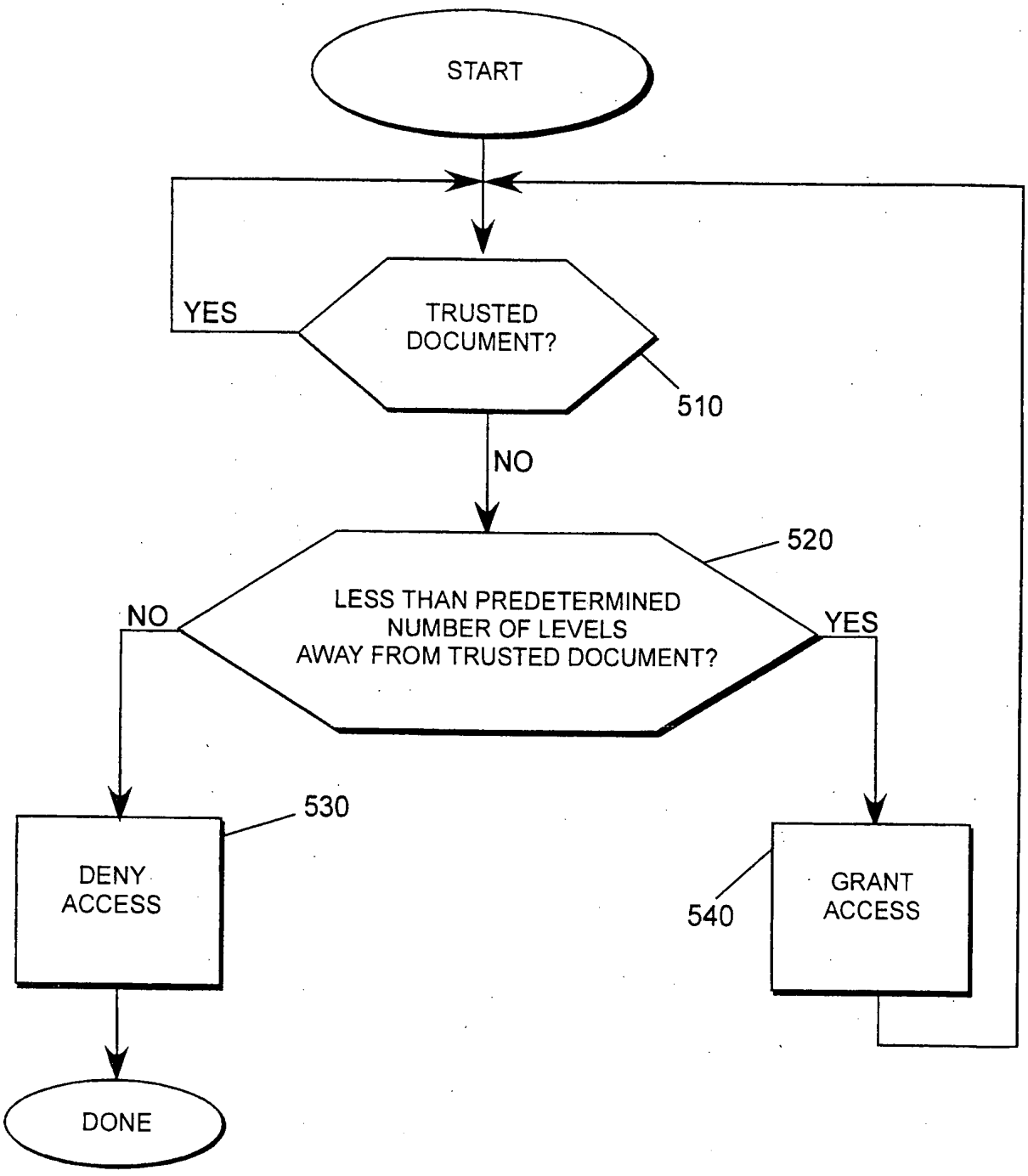


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/25573

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :Please See Extra Sheet.
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/51, 52, 59, 67, 76; 709/227, 228, 229, 311, 313; 713/200, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P ---- Y,P	US 5,996,011 A (HUMES) 30 NOVEMBER 1999, COL. 2, LINES 48-51, 54-55, 59-62, COL. 3, LINES 1-3, 10-22	1-3, 5-10, 12-21 --------- 1-3, 5-10, 12-21
Y,P	US 6,092,194 A (TOUBOUL) 18 JULY 2000, SEE ENTIRE DOCUMENT	1,8,15,18
Y	US 5,784,564 A (CAMAISA ET AL) 21 JULY 1998, SEE ENTIRE DOCUMENT	1,8,15,18
Y	US 5,706,507 A (SCHLOSS) 06 JANUARY 1998, SEE ENTIRE DOCUMENT	1,8,15,18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 30 OCTOBER 2000	Date of mailing of the international search report 04 JAN 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Hamrod CHRISTOPHER A REVAK Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/25573

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (7):

G06F 9/00, 9/46, 11/30, 12/14, 15/16, 15/163, 17/60; H04K 1/00; H04L 9/00, 9/32

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

705/51, 52, 59, 67, 76; 709/225, 226, 227, 228, 229, 311, 313; 713/200, 201

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS (USPAT, DERWENT, JPO, EPO, IBM TDB'S), DIALOG (FILE COMPSCI), ACM, CORPORATE RESOURCE NET

search terms:
resource, file, electronic, executable, downloadable, applet, trust, trusted, trusting, entrust, entrusted, entrusting, program, software, license, licensed, page, document, object, safe, secure, signed, signature, certified, certificate, count, counter, counting, number, track, times, access, execute, run, open, occurence, link, allow, deny, reject, accept, discard, erase, permit